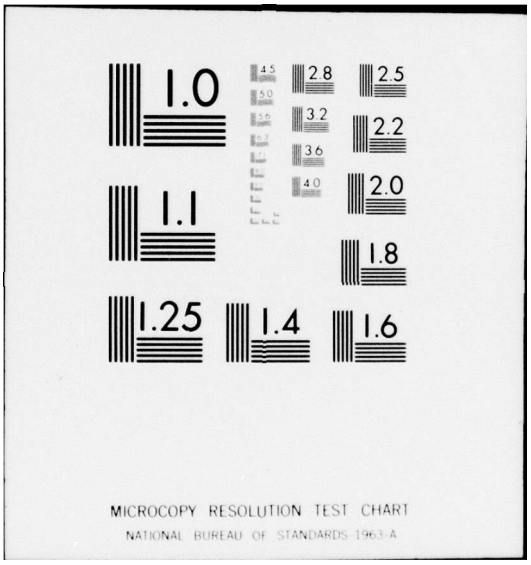
AD-A037 897 RAND CORP SANTA MONICA CALIF F/G 5/11
PRIVACY ISSUES AND THE PRIVATE SECTOR,(U)
JUL 76 W H WARE
UNCLASSIFIED P-5685 NL

1 OF 1
ADA037 897

END

DATE
FILMED
4-77


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

(2) B.S.

(12) 17 p.

(6) # PRIVACY ISSUES AND THE PRIVATE SECTOR

(10) Willis H. Ware

(11) July 1976

(14) P-5685

296 600

The Rand Paper Series

Papers are issued by The Rand Corporation as a service to its professional staff. Their purpose is to facilitate the exchange of ideas among those who share the author's research interests; Papers are not reports prepared in fulfillment of Rand's contracts or grants. Views expressed in a Paper are the author's own, and are not necessarily shared by Rand or its research sponsors.

The Rand Corporation
Santa Monica, California 90406

PRIVACY ISSUES AND THE PRIVATE SECTOR

It is a choice opportunity to address an audience representing the diversity of interests, and of corporations and business in this country. This is a group important to address on the subject of privacy. GUIDE represents a large portion of the private sector of this country; at the moment, of course, the recordkeeping processes of non-Federal organizations are being examined for possible legislative safeguards.

As professional individuals you not only specify but design, implement, and operate systems that deal with much information about people, and especially much information that is identifiable to the individual. As such, therefore, each of you has to be concerned with a major social issue that has a very intense technological component.

Information about people has always been used for some purpose; that per se is not new. It has always been used to make determinations and judgments about rights, privileges or benefits that an individual might have, but there is something different. There is today a vast amount of information about each one of us in record systems. Much of it, to be sure, is in manual systems, but much of it is in computerized systems for which we as an industry have been responsible. Moreover, the records that do exist in computerized systems are much more complete and the scope of their content about us is much more extensive. Thus, it is the scale and extensiveness of recordkeeping that is different from twenty-five years ago; of course the modern day computer has made it possible.

This is the keynote address to the GUIDE meeting in Washington, D. C. on May 26, 1976, by Willis H. Ware.

The trend will probably continue even more extensively; there are continuing signs of it. For example, the credit granting industry is always interested in opening up new areas for credit; when the margin of error for a poor decision is large, decisions will have to be sharp and crisp. More information about people will be needed to make proper credit judgments. When information about people becomes extensively used in making determinations about them, there are inevitably opportunities for misuse; there are opportunities for using it in ways to harm individuals. Furthermore, organization motivations can prevail over intentions to treat people fairly and humanely.

Information in modern day record systems is used directly to affect our lives; each of us knows it. It can be used to preempt individual behavior and to cause people to make decisions or take actions that might have been different given a free choice. Information is being used to control our choices about trivial things, and to control our choices about moral things sometimes. We behave differently simply because of the existence of such systems. The totality of information about people residing in record systems has become a significant and pervasive influence; it has become even an intrusion into our personal autonomy.

Nonetheless, I cannot help but be convinced the future will be one in which information about individuals will be used even more extensively than it is today, and in very broad ways. In brief, the argument is as follows. We as a society levy heavy demands upon government for services. This results in extensive social programs that not only have to be administered, but monitored as well. That all adds up to information about people, and it is not likely to get less. This is a big country: 225 million people leading

very complex lives, creating substantial data trails every day. Just to make the country work much information about people is essential. It is clear that our planning processes will have to get better. It is clear that we will always have to strive for efficiency in government. It is clear we will have to do an ever-improving management of the limited resources we have on the planet. There are corresponding effects, of course, in the private sector: conduct of business, efficiency of business, product planning, service planning, service distribution, response to Federal and State laws. This all implies recordkeeping, with people as the prime subject.

To me it all points to an inevitable future in which both the public and private institutions in this country will require information about people in ever-increasing amounts. Of course, the essential thing is to make sure that ~~we have~~ a proper balance between such legitimate needs and adequate safeguards that can protect ~~each one of us~~ individuals against harm as a result of the existence of record systems.

It is well and good to point out the way of the future, but why is there an issue? Why is there contemporary concern about all of that?

First, there is no broad legal basis for the ownership of personal information. In isolated instances, the case is clear; for example, under California law, medical records are the property of a hospital. When one of us gives information freely or compulsorily by law, there is no ground on which to assert that we continue to own it and therefore can continue to control it. Hence the holder of the information does with it as it sees fit, and especially it uses information as the motivations of the organization require. Expedience, payoff, profit or even the desire of an organization

preempts in most cases concern about the individuals which are the subjects in a record system. Thus the holder of information about people does not normally consult the data subject in the use of information.

Prior to the Privacy Act of 1974, recordkeeping systems tended to be largely secret, not because there was a positive action to keep them so, but rather because there was no particular motivation to make them visible. Especially the recordkeeping activities of the Federal Government were largely unseen by the public. While the Act has caused much to surface, even today it would be a major task, if not an overwhelming one, to discover which agencies of Federal government have records about any one of us. In the private sector, of course, it is yet an impossible task, because much of its recordkeeping has yet to become publicly visible. Furthermore, prior to the 1974 Act, there was no mechanism whereby an individual could cause a Federal record about himself to be examined, to be challenged, and if in error to be corrected. The 1974 Act has created a mechanism for just the purpose as the Fair Credit Reporting Act did previously for credit bureau records. Even if one can find a record system that holds information about himself in the private sector, he may or may not have access to that. To the extent one does, it is at the pleasure and voluntary compliance of the private organization concerned. A final aspect of concern is simply that the bulk of personal material about any one of us is unprotected by law and subject to court seizure; thus one hears incidents in which the record of some person has been subpoenaed for some process, and suddenly it will appear in full public view.

Thus, we find that personal information tends to circulate very freely today. It tends to be collected as the recordkeeper wishes, to be used largely as the recordkeeper wants and to serve purposes as he sees fit. His uses are not necessarily in the best interest of the data subject, and so there is a one-sided situation today between any one of us and all the record systems that surround us. So to speak, we are on the short end of the stick. The unbalance has been exaggerated by the discovery in some private organizations that information as a commodity is profitable. We are seeing a whole new industry develop in which the commodity of concern is information about individuals.

Because of the one-sidedness of the situation, because of the lack of legal protection, and because of the lack of a legal basis for ownership, there are opportunities for misuse or abuse of personal information, with the conseqeunce that an individual or a group of individuals or some segment of society can be harmed in some fashion or improperly denied an opportunity or benefit.

With that as a background, I would like to note that the privacy issue is forcing the country and its institutions into a very thorough reexamination of recordkeeping practices. It is forcing every organization to look very carefully at procedures and practices that have largely evolved and probably without much overall guidance; rather they have been created without a total system view for an organization and certainly without design goals that stipulated safeguards and concern for the individual. Organizations will have to ask very subtle and searching questions. For example, we as a society will probably have to come to grips with the question: "What will we view as socially acceptable uses of information about any one of us?" We will have

to answer the question: "What information about people will we as a society allow to be collected?" As a country we are searching for an appropriate public policy to govern the use of information about people.

There is a beginning; even now certain questions may not be asked a person on employment questionnaires. We will have to establish a public position on many aspects of information usage; privacy happens to be one of the first.

Every member of society will have to acquire an information awareness in the coming generation. So to speak, the information IQ of each of us will simply have to get better. We will have to become as familiar with information--its uses, its dissemination, its migration, circulation--as we now are comfortable with automobiles.

Of course in the middle of all this prominent social issue is the technology that you and I both represent--a computer technology that just has to be one of few most important ones to the world. Certainly it is unique in that it affords man the only way to process information faster than by his brains.

There are two subjects that overlap, but are different. They need to be distinguished carefully: computer security and privacy. The following definitions seem to represent the present usage. Computer security: It is the totality of measures or safeguards that are required to first protect a computer-based system, including its physical facilities, its personnel, and its data, against deliberate or accidental damage from a defined threat. Note that one is not protecting the system against all threats imaginable,

but only against the threat that its owners and operators perceive. Secondly, it is the totality of measures that protect the system against denial of use by rightful owners. For example, the FEDWIRE network is a nationwide communication data system that the Federal Reserve Bank uses to exchange bank payments. Can you imagine the chaos if the FEDWIRE were preempted for even a day by a dissident group? Finally, security includes the set of safeguards that protect the system's data and its processing capability against use by unauthorized persons. Security is largely a technical matter--partly one of hardware and partly of software--but it also has administrative and procedural aspects as well.

In contrast, however, privacy is quite a different thing. For one thing it is a very troublesome word, but in the context of record systems it means the following: It is the view of the individual (or of groups of individuals or of institutions) to determine for themselves when, how and to what extent data about them is communicated to or used by others. This is the notion of control, that an individual in some way should be able to control how information about him is used. The second aspect of privacy is that of protecting an individual against harm or damage as a result of the operation of a record system. The third is the collection aspect--that of protecting an individual or class of individuals against unwelcome, unfair, improper or excessive collection or dissemination of information. These three are the prominent aspects of the total privacy question as it is being examined today. The protection part needs elaboration.

There are two possibilities to be identified with care. The obvious one is that in which the determination about the individual is unfair for some reason. It was based on incomplete information; it was based on stale

information; it was based on irrelevant information; and a reasonable person would have said: "Yes, it is unfair and inappropriate." This circumstance is properly regarded as a privacy abuse, but there is the counter circumstance in which a negative but legitimate decision is made about an individual. The facts--complete, accurate, timely and relevant--do in fact support a negative position--denial of credit, for example. A legitimate but negative decision about an individual cannot be regarded as a privacy abuse.

There is another aspect of the harm-and-abuse facet that is worthy of attention. It has been called stigmatization. A corporation--for example, an insurance corporation--may decide to discontinue underwriting insurance in a certain geographical region for reasons of its own; it is a corporate decision based on portfolio management. It may wish to spread its risks differently or to geographically spread its policyholders differently; it may simply discontinue writing insurance for some calendar period. Unfortunately an individual in the affected area who applies for insurance will be declined, but the declination typically will not reveal why. It will simply reveal that individual "A" did not get insurance with Corporation "X", with no reason stated. Therefore, when that individual turns to the next insurance company, he is at a disadvantage because he already has a declination on his record.

The point I make is that a private company can make a decision for corporate reasons that will impact an individual indirectly. The decision made by the corporation had nothing to do with any individual. It was not an explicit determination about him, but he will have been "stigmatized" inadvertently.

This circumstance is the first aspect of privacy to appear that is unique to the private sector. There seems to be no analog of it in government. Thus, it is of special interest to us who are studying the recordkeeping practices of private industry.

The privacy issue started to come into focus with well known books by Allen Westin, Arthur Miller and Jim Rule. It achieved significant impetus from a committee chartered by Secretary Elliot Richardson, then of DHEW, who pointed the group toward an examination of the recordkeeping practices of his agency. The ensuing report, published in July of 1973, has had a profound effect on the privacy issue in this country and to some extent in the world. Over 10,000 copies of it now are in circulation; the familiar red book with a big blue dot in the center of its cover has become a well known volume. "Records, Computers and the Rights of Citizens" has set the tone, concepts and even the language for most legislative attempts to treat privacy in an omnibus fashion. The report made several very important contributions.

First, it did define privacy in terms of mutuality of interest between recordkeeper and data subject. Secondly, it introduced the notion of "fair information practice" as a basis for improving the balance between record-keeper and data subject and as a means of assuring mutuality of interest and joint control. It set forth five general principles which are regarded as the foundation for privacy safeguards. Finally it suggested features that a code of fair information practice might contain. Language and concepts were lifted from the report with minimal change and became the basis for omnibus legislative attempts in the country.

For example, the Federal Privacy Act is based on the concepts, principles, and even language introduced by the HEW report; many state efforts also are. It is to be noted that there are other ways to provide privacy safeguards; an obvious one is target legislation on a particular problem. The Fair Credit Reporting Act is one example; the credit reporting industry was perceived by Congress to be troublesome, and legislation was levied against it. The Fair Trade Billing Act is also an example. In contrast an omnibus approach throws a broad blanket of general safeguards over an entire government or over an entire country.

The legislation that we know as the Privacy Act of 1974, Public Law 93-479, culminated roughly eighteen months after publication of the HEW report. It provids safeguards for the citizens, specifies a standard of behavior for recordkeeping, and includes both criminal and civil sanctions that a data subject can invoke against a record system. The Fair Credit Reporting Act predates the Privacy Act; there are similar features in both to examine and contest a record. The HEW report surely used ideas that were already present; its "five principles" are concise restatements for other concepts. On the other hand, its comprehensive treatment of the subject and its "Code of Fair Information Practice" were strong stimulants to catalyze action by Congress.

Earlier drafts of the Privacy Act included both Federal Government and private sector. Fortunately, the final version of the Act applied only to the Federal sector, but Section 5 created the Privacy Protection Study Commission to examine the private sector and non-Federal government. The Commission is to recommend to Congress and the President first, what aspects of the 1974 Act should be applied to the private sector, and parenthetically

I would stress "if any"; secondly, to recommend to Congress and the President what further legislative safeguards are indicated for the private sector.

The Commission, which began its life in June of 1975, will expire in June of 1977. It is composed of seven people; two are appointed by the Senate, State Senator Robert Tennessen, responsible for the Minnesota Privacy Law, and retired newspaper editor William Dickenson. Two are appointed by the House, Congressman Goldwater, Jr. of California, and Congressman Koch from Manhattan; they of course were the prime movers behind the 1974 Act in the House and are the authors of an Act bearing the fascinating label, "HR 1984." The last three members of the seven were appointed by the White House; Mr. William Bailey, president of Aetna Life and Casualty Insurance Company, Mr. David Linowes, a partner of a management consulting firm in New York City, and myself. Among the seven a rather broad range of skills is represented: the legislative process at both State and Federal levels, law, business management, media, business accounting, business auditing, business practices, and of course data processing technology.

The law specifies a lengthy list of topics that could take several years and several million dollars; we have two years and $1.5 million. It specifies that we "shall" do some things and we "may" do other things. Broadly speaking, our goal is to look at the recordkeeping practices of the country, excluding the Federal Government, to understand those recordkeeping practices, to perceive not only present opportunities for privacy abuses but future ones as well, and of course make appropriate recommendations to the Congress and to the President. We have a few special collateral issues to examine. One is to look at the mailing list problem: should an individual be able to get his name removed from a mailing list? The second is to examine the

question of sharing Federal tax information with state and local levels. The third, as you might anticipate, is the universal personal identifier and the role of the Social Security number in that regard.

To do our task we are holding hearings every month on some segment of industry. We have, for example, looked at the mailing list industry; we have looked at the credit card industry and at hotels and reservations and at airlines. We have looked at credit granting and at depository and lending institutions. In May we heard the insurance industry, and in June we will look at health records. In the future are credit reporting, personnel systems, statistical systems, and others. Our staff of approximately 20 is more than busy keeping the schedule of hearings going. We will have only six months of 1977 to run, so we must digest all of what we have learned and establish our position and write a report in the first few months of 1977.

The Privacy Protection Study Commission is being watched by everyone in the country that is interested in the issue. It is the forum in which the matter is being examined in a structured and considered way. It is the place to which one must turn his attention if privacy is of concern to him.

Let me divert for a moment to talk about costs, an ever-important question. I will express what may strike you as a cavalier attitude toward cost at the Federal sector. The argument I would make is as follows: The estimates of the cost of privacy are enormously varied. They are not based on considered analyses, nor on real experience; they are the softest kind of numbers. Nonetheless there is some chance that figures of $200-300M are more or less right--or they might even be right. If they are, I would argue

as follows: Over 200 million people live in this country, so the cost of privacy is $1-2 apiece; and I submit that is a good buy. I would note in perspective that the country has agreed to underwrite costs which are significantly greater than that on a per capita basis. We spend $10 or $12 apiece per year on the pollution problem. We have spent in the last many years something like $10 or $12 apiece on the national highway system. We have put something more than that amount into the Apollo Moon Programs; annually we spend several hundred dollars apiece in the defense establishment and many hundreds of dollars apiece in HEW.

The point I want to make is that even several hundred million dollars, while large in an absolute sense, is a readily acceptable cost to pay for privacy safeguards at the Federal level. I cannot and would not make a corresponding argument at the local level; I would not even attempt to suggest such an argument for private industry. In the latter instances the cost picture is even softer, but the base over which one wishes to spread it is even smaller. Therefore, it is conceivable to me that the cost question at state or local level may prove very serious; it might be devastating in some parts of private industry. Cost is a large unknown but it is obviously a facet that has to be of concern to us as a Commission; as we try to make judgments among what appears to be good ideas for privacy safeguards, we must consider the cost of imposing them.

An important thing has happened as a result, I think, of the existence of the Commission and of the public visibility it has received. Our meetings are open, and anyone who attends will find it interesting and will learn something he didn't know. Each morning something new surfaces about the

use of personal information and the way it gets from here to there and migrates about. Importantly, the very existence of the Commission has caused organizations to voluntarily consider things that have been dormant.

Speaking for myself, I was generally a disbeliever in voluntary compliance as of late 1975. I felt that the problem is so diffused and so pervasive that voluntary compliance and voluntary codes of ethics probably would not work. Moreover, I was also a disbeliever in a Federal privacy board because I was unconvinced that the problem called for one. Interestingly there have been very rewarding and spontaneous responses from companies. Sometimes it is the result of questioning by Commissioners, but frequently a company simply as a result of observing the social standard have voluntarily examined their internal recordkeeping practices and are taking rather vigorous remedial actions. Our hearings bring people together to talk about a problem. Not only is that rewarding, but it is also valuable because it will act to avoid legislative safeguards that might prove inappropriate later.

To my view, what the Commission has to do is to start ab initio and to very carefully inquire: "Are the principles laid down in the HEW report, and obviously relevant at the Federal Government level, also relevant to the private? If they are, how are they relevant? What are the privacy issues? Are the privacy issues such as they may be--collection, use, dissemination--of sufficient importance that remedial action is warranted." If remedial action is warranted, what are the right safeguards? What are the costs of those safeguards? We do not have an easy task to arrive at a carefully considered rational position.

You and I--each one of us is a responsible member of the data processing industry. As such, we must realize that it is an industry that will change

the world in ways the world has never been changed; we probably have seen so far only a small part of what will eventually come vis-a-vis the impact of computer technology and data processing on the conduct of the affairs of people, the affairs of government, and the planet in general. We must be concerned about the impact of our work, because computers and data processing play such a pivotal and pervasive role in the affairs of the world.

I would urge you to be involved simply because you are a professional individual in an essential technology that is effecting the world. I would also remind you that you--as I--are in record systems as a data subject; as an individual of the country you should hold the same concerns about the content of your records, about its use, about the determinations that information influences; you must be alert to how that information flows from place to place; how it gets into the hands of law enforcement agencies; how it gets from Federal to State level. Each such thing must be of concern to you simply as an individual in this country.

Finally, I think you must be involved as members of a responsible organization like GUIDE that encompasses a significant portion of private industry. GUIDE must itself consider a position that it might wish to take; it can influence and help the country move forward and find an appropriate balance point between recordkeeping systems and individual. I will say it to you strongly. If we, the Commission, and by implication the legislative process of the country, do not hear from you, then the decisions that we will make will have to be ones that seem to us best on the basis of our perception of the circumstances. Certainly we will do our best to get the most accurate perception, but it may not be a complete perception.

Therefore we need to hear from you. If we do not, it will be an embarrassing situation when I talk to you some years from now. You will complain about something you do not like and my response will have to be, "I'm sorry; you didn't speak up. We did the best we could on the information we had, but we didn't hear from you." I wouldn't want to take such a position; you wouldn't want me to have to take it. Therefore I would urge that you do your utmost as individuals, as members of GUIDE, and as responsible employees of companies, to be informed on the privacy issue, to urge your companies to take whatever steps are appropriate internally, vis-a-vis voluntary compliance, and to contribute as you can.